METHOD FOR SECURELY PROVIDING ENCRYPTION KEYS

ABSTRACT OF THE DISCLOSURE

Method for securing encryption keys for encrypting software while providing for secure updates of the key for other or updated versions of the software. A First Encryption Key which is used to encrypt an initial software version includes a FIRST SPLIT portion and a TOKEN portion. The FIRST SPLIT portion can be stored in an anti-tamper storage memory of a hardware product and the TOKEN can be stored in external storage medium so that the FIRST SPLIT and the TOKEN are separately provided to separate personnel of the user while the identity of the First Encryption Key is kept secure by remaining in custody of the provider. The user employs the hardware to combine the FIRST SPLIT and TOKEN to generate the First Encryption Key within the hardware to decrypt the encrypted software. To facilitate updates the provider combines the First Encryption Key with a Second Encryption Key to generate an UPDATE SPLIT for updated software which is encrypted with the Second Encryption Key. The UPDATE SPLIT and encrypted updated software are provided to the user who employs the hardware to calculate the Second Encryption Key from the FIRST SPLIT, UPDATE SPLIT and the TOKEN. This allows the identity of the Second Encryption Key to also remain secure in the custody of the provider. The Second Encryption Key which can be sequential or non-sequential with the First Encryption Key, is used within the hardware product to decrypt the encrypted updated software.